Penetration Test Report

FAKE Consulting Group

01 AUG 2017

Security Department Services

www.securitydept.com

sales@securitydept.com

Penetration Report - FAKE Consulting Group

1. EXECUTIVE SUMMARY 3
1.1 SUMMARY 3
1.1.1 Approach 3
1.1.2 Scope of work 3
1.1.3 Project Objectives 3
1.1.4 Timeline 3
1.1.5 Summery of Findings 4
1.2 METHODOLOGY 4
1.2.1 Planning 4
1.2.2 Exploitation 4
1.2.3 Reporting 5
2 SUMMARY OF RESULTS 6
2.1 SYSTEM DENIAL OF SERVICE 6
2.2 EXPONENTIAL ENTITY EXPANSION DENIAL OF SERVICE 6
2.2 USERNAME ACCOUNT LOCKOUT 7
2.3 XML INJECTION 8
2.5 INFORMATION LEAKAGE?? 9
3 CONCLUSION 10
4 REFERENCES 10

Penetration Report - FAKE Consulting Group

1. Executive Summary

1.1 Summary

Security Department Services was contracted by FAKES Consulting Group to conduct a penetration test on Public web Service in order to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against FAKES Consulting Group with the goals of:

- Identifying if a remote attacker could penetrate FAKES Consulting Group's defenses to determining the impact of a security breach on Service.
- Confidentiality of the company's private data
- Internal infrastructure and availability of FAKES Consulting Group's information systems

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in OWASP Testing Guide with all tests and actions being conducted under controlled conditions.

1.1.1 Approach

- Review web service documentation to identify targets
- Preform target scans and manual investigations to identify vulnerabilities and additional targets
- Identify and validate vulnerabilities and rank risks
- Document details
- Transfer knowledge

1.1.2 Scope of work

White/Black box application penetration test limited to one week and one web service test site

1.1.3 Project Objectives

The security assessment is carried out to evaluate the security posture of the FAKES Consulting Group public soap service. Given the limited time of the assessment only services that identify as risky are given extra attention.

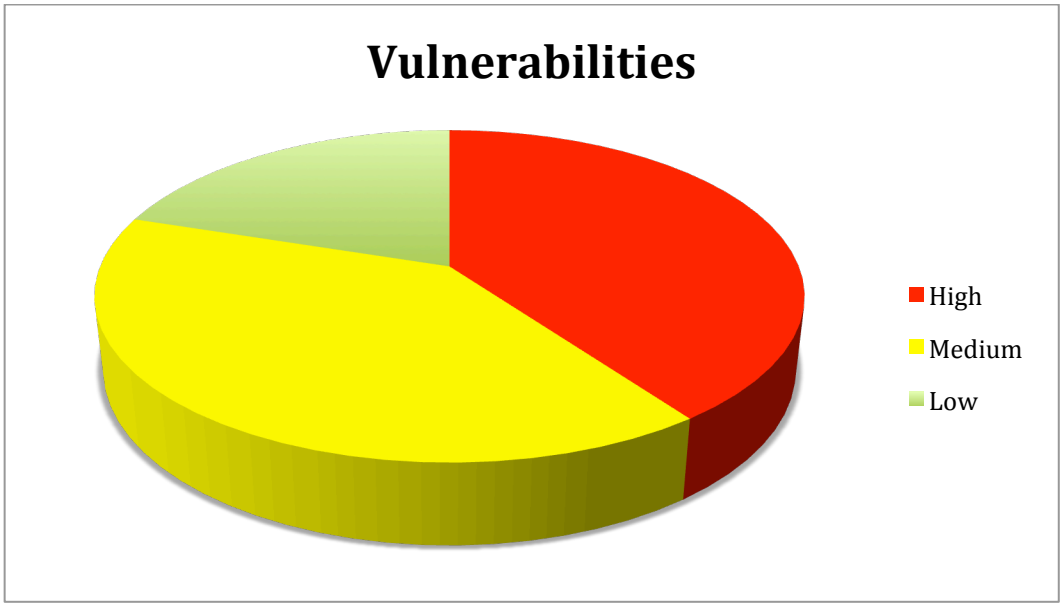
1.1.4 Timeline

	Start Date/Time	End Date/Time

Discover	8/15/17	8/15/17
Testing	8/15/17	8/19/17
Reporting	8/19/17	8/22/17

1.1.5 Summery of Findings

	Number of findings
High	2
Medium	2
Low	1



1.2 Methodology

1.2.1 Planning

During the planning stage we are identifying targets to test and determining attack scenarios

1.2.2 Exploitation

Utilizing what was learned in the planning stages we execute the specialized tests to determine if the service is vulnerable to a given attack

1.2.3 Reporting

Based on the results of 1.2.1 and 1.2.2 we analyze the results and assign a risk

2 Summary of Results

2.1 System Denial of Service

Risk	High
Classification	Denial of Service
Link	https://www.owasp.org/index.php/Denial_of_Service
Resource	*
Analyst	Sending 1 messages will cause the soap service test site to stop accepting requests
Recommendations	Determine cause of system failure and correct or mitigate
Evidence/Example	Image/Documation/Raw Request

2.2 Exponential Entity Expansion Denial of Service

Risk	High
Classification	Exponential Entity Expansion Attack (Billion laughs)
Link	https://en.wikipedia.org/wiki/Billion_laughs
Resource	*
Analyst	Sending 1 messages pre connection thread will cause the soap service test site to stop accepting requests
Recommendations	Determine cause of system failure and correct or mitigate
Evidence/Example	Image/Documation/Raw Request

2.2 Username Account Lockout

Risk	Medium
Classification	Account Lockout
Link	https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks
Resource	*
Analyst	Sending 3000 login request should cause the user account to be locked out
Recommendations	Create a reasonable lock out system that will disable accounts before CATS words can be brute forced
Evidence/Example	N/A

2.3 XML Injection

Risk	Medium
Classification	XML Injection
Link	https://www.owasp.org/index.php/Testing_for_XML_Injection_(OTG-INPVAL-008)
Resource	*
Analyst	Xml injection can lead to bigger problems like XXE we did not observe any XXE in this case but more testing or a code review on the given XML parsing code would be needed
Recommendations	Sanitize all input and validate before executing xml data
Evidence/Example	Image/Documation/Raw Request

2.5 Information Leakage

Risk	Low
Classification	Information Leakage
Link	https://www.owasp.org/index.php/Information_Leakage
Resource	*
Analyst	Leaking of exception data expose Sensitive information that could assist hackers in exploiting systems, please note we were able to get this to fire a few times, it seams sporadic
Recommendations	Sanitize all exception data delivered to caller creating alternate privileged error/exception channel would also mitigate
Evidence/Example	Image/Documation/Raw Request

3 Conclusion

In order to maintain a high level of security posture continuous penetration testing must be completed yearly, or when major changes to the affected infrastructure or software have taken place. Correcting the findings in this report will improve the security posture of the application as a whole. It is recommended to conduct a full code review of your base Service in order to determine further areas of improvement.

4 References

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=Main

